Dyrektywa 2016/680 w praktyce krajowej: gdzie kończy się implementacja, a zaczynają problemy systemowe? (cz. II)

Posted on 2026-04-30

W marcowym numerze Biuletynu UODO przedstawiliśmy systemowe problemy związane z zakresem wyłączeń w wymiarze sprawiedliwości oraz modelem nadzoru nad przetwarzaniem danych osobowych przez sądy i prokuratury w Polsce. Niniejsza część koncentruje się na praktycznym funkcjonowaniu instrumentów przewidzianych w dyrektywie 2016/680, w szczególności na uprawnieniach organów nadzorczych, modelu sankcyjnym oraz realizacji praw osób, których dane dotyczą.

Dyrektywa 2016/680 w praktyce krajowej: gdzie kończy się implementacja, a zaczynają problemy systemowe? (cz. II)

Ewaluacja wdrożenia Dyrektywy 2016/680 w Polsce po raz kolejny wykazała, że mimo formalnej transpozycji przepisów ich skuteczność jest ograniczona przez bariery proceduralne, niejednoznaczny zakres kompetencji oraz niepełne wykorzystanie dostępnych instrumentów.

Uprawnienia Prezesa UODO w zakresie prowadzenia postępowań należy co do zasady ocenić jako funkcjonalne i wystarczające. Pracownicy Urzędu, działający z jego upoważnienia, mają możliwość wglądu do danych oraz dokumentacji związanej z kontrolą, a także pozyskiwania informacji niezbędnych do monitorowania i egzekwowania przepisów ustawy wdrażającej dyrektywę 2016/680, w tym w postępowaniach skargowych.

Uzupełniająco Prezes UODO może zwrócić się do inspektora ochrony danych o przeprowadzenie sprawdzenia zgodności i przedstawienie sprawozdania z jego wyników.

Nie odnotowano sytuacji, w których brak dostępu do danych uniemożliwiałby prowadzenie postępowania w trybie DODO.

Prawo pośredniego dostępu do danych

W polskim systemie prawnym brakuje mechanizmu pośredniego dostępu do danych, który umożliwiałby osobie, której dane dotyczą, skorzystanie z dodatkowej gwarancji ochronnej w przypadku odmowy udostępnienia informacji, sprostowania lub usunięcia danych przez organy ścigania. Obywatel nie może zatem zwrócić się do Prezesa UODO o przeprowadzenie niezależnej weryfikacji legalności przetwarzania danych w tym obszarze. W praktyce oznacza to pozbawienie jednostki możliwości skorzystania z jednego z kluczowych instrumentów ochronnych przewidzianych w dyrektywie 2016/680, a tym samym osłabienie prawa do skutecznego środka ochrony prawnej.

Argumentacja polskiego ustawodawcy, zgodnie z którą funkcję tę miałoby realizować prawo do wniesienia skargi, nie jest trafna, zważywszy na komplementarny, a nie zastępczy charakter obu instrumentów. W projekcie ustawy wdrażającej DODO przedłożonym w 2018 r. projektodawca wskazywał, że mechanizm przewidziany w art. 17 dyrektywy 2016/680 ma być realizowany za pośrednictwem skargi do Prezesa UODO, o której mowa w art. 52 tej dyrektywy. Prezes UODO od początku podnosił jednak, że są to odrębne instrumenty prawne, realizujące odmienne cele i wymagające odrębnych procedur. Stanowisko to zostało potwierdzone w orzecznictwie Trybunału Sprawiedliwości UE (wyrok w sprawie C-333/22).

W konsekwencji należy stwierdzić, że w prawie polskim – w odróżnieniu od 23 państw członkowskich UE – art. 17 dyrektywy 2016/680 nie został skutecznie wdrożony. Do

analogicznych wniosków doszli również ewaluatorzy przeprowadzający w 2024 r. ocenę stosowania przez Polskę dorobku Schengen. W wyniku Ewaluacji Schengen Polska została zobowiązana do usunięcia stwierdzonych nieprawidłowości oraz do zapewnienia, aby osoby, których dane dotyczą, mogły wykonywać swoje prawa dostępu, sprostowania i usunięcia danych osobowych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym za pośrednictwem Prezesa UODO w przypadku odmowy realizacji tych praw przez właściwe organy.

Czego najczęściej dotyczą wnoszone skargi

W obszarze realizacji prawa do wniesienia skargi w obszarze ochrony porządku publicznego obserwuje się w Polsce umiarkowaną, zasadniczo stabilną liczbę spraw kierowanych do organów nadzorczych w latach 2022–2025. Na tle państw UE Polska nie należy do jurysdykcji o najwyższej liczbie skarg – rozkład w Unii jest silnie zróżnicowany – jednak skargi pozostają w Polsce istotnym źródłem sygnałów o nieprawidłowościach w przetwarzaniu danych w sektorze operacyjnym.

W sprawach pozostających w zakresie właściwości Prezesa UODO dominowały skargi dotyczące funkcjonowania policyjnych systemów informacyjnych, w szczególności Krajowego Systemu Informacyjnego Policji, a także – w mniejszym zakresie – Krajowego Centrum Informacji Kryminalnych oraz Centralnej Bazy Osób Pozbawionych Wolności. Wśród najczęściej podnoszonych zarzutów pojawiały się kwestie udostępniania danych osobom nieuprawnionym, przetwarzania danych po upływie ustawowych okresów retencji, braku podstawy prawnej przetwarzania lub udostępniania danych, niewykonywania obowiązków informacyjnych wobec osób, których dane dotyczą, a także odmów usunięcia

danych w systemach. Odnotowywano również skargi związane z udostępnianiem danych przez podmioty penitencjarne (w tym sytuacje, w których dane miały trafić do innych osadzonych) oraz przypadki dotyczące udostępniania danych w toku czynności policyjnych.

Z perspektywy proceduralnej znaczenie ma także to, że część skarg nie mogła być merytorycznie rozpoznana z przyczyn formalnych (np. z uwagi na ich wniesienie po przewidzianym terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora), co w konkretnych sprawach przekłada się na ograniczenie możliwości uzyskania rozstrzygnięcia co do meritum.

Odnotowano ponadto skargi wnoszone przez straże miejskie, które dotyczyły odmowy udostępnienia danych przez operatorów telekomunikacyjnych lub zakłady ubezpieczeń, co – w ocenie skarżących – utrudniało ustalenie sprawców wykroczeń. Pokazuje to, że spory na tle DODO mogą dotyczyć nie tylko nieprawidłowości po stronie organów, ale również praktycznych barier w pozyskiwaniu danych w ramach czynności służbowych, wymagających każdorazowo oceny podstaw prawnych i zasadności żądania.

W zakresie właściwości organów nadzorczych funkcjonujących w strukturach prokuratur wskazywano skargi odnoszące się m.in. do ujawniania danych w treści rozstrzygnięć wydawanych w postępowaniach przygotowawczych, braku anonimizacji danych w aktach spraw karnych, gromadzenia materiałów zawierających dane genetyczne oraz realizacji praw dostępu i usunięcia danych. Jednocześnie podkreślano, że w odniesieniu do danych przetwarzanych w ramach postępowań karnych wykonywanie praw osób, których dane dotyczą, bywa w praktyce ograniczone do zakresu wynikającego z przepisów szczególnych regulujących przebieg tych postępowań, a nie na podstawie ustawy grudniowej.

Powiadomienia o naruszeniach ochrony danych

Prezes Urzędu Ochrony Danych Osobowych odnotowuje sytuacje, w których administratorzy danych nie przekazują organowi informacji o naruszeniu ochrony danych w terminie 72 godzin od jego stwierdzenia, powołując się na trwające czynności operacyjne lub konieczność zachowania poufności zdarzenia. Choć obowiązek zgłoszenia powinien być zrealizowany niezwłocznie po ustaniu przeszkód wraz z wyjaśnieniem przyczyn opóźnienia, w praktyce zdarza się, że Urząd otrzymuje te informacje ze znacznym opóźnieniem. Bywają także przypadki całkowitego odstąpienia od zgłoszenia. Powoduje to istotne ograniczenia w dostępie do danych i informacji wymaganych do prowadzenia postępowań i pełnej oceny skali naruszeń.

Model sankcyjny

Istotnym problemem pozostaje brak skutecznych sankcji o charakterze odstraszającym. W obecnym modelu Prezes UODO nie ma możliwości nakładania administracyjnych kar pieniężnych za naruszenia przepisów tej ustawy, a jednocześnie nie dysponuje także „miękkim” instrumentem prewencyjnym w postaci upomnienia (analogicznego do rozwiązania znanego z RODO). Oznacza to, że postępowania mogą tracić walor oddziaływania prewencyjnego: nawet jeśli naruszenie zostanie stwierdzone, a następnie usunięte, organ nie ma do dyspozycji środka, który w sposób wyraźny „zamyka” sprawę

konsekwencją o charakterze wychowawczym lub odstraszającym.

Jednocześnie należy zauważyć, że organy nadzorujące ochronę danych osobowych w sądach i prokuraturze posiadają możliwość stosowania upomnienia, podczas gdy Prezes UODO – jako organ o najszerszej roli systemowej – takiego narzędzia nie ma. Z perspektywy spójności i skuteczności systemu nadzoru osłabia to jednolity standard reakcji na naruszenia w obszarze objętym DODO i utrudnia realizację wymogu, aby sankcje były „skuteczne, proporcjonalne i odstraszające".

Wnioski

Praktyka stosowania przepisów wdrażających dyrektywę 2016/680 jednoznacznie wskazuje, że główne problemy mają charakter systemowy. Formalna implementacja nie przekłada się w pełni na skuteczną ochronę praw jednostki, w szczególności w warunkach ograniczeń proceduralnych i niepełnego wykorzystania dostępnych instrumentów.

Istotną luką pozostaje brak mechanizmu pośredniego dostępu, co oznacza niepełną implementację dyrektywy i osłabienie prawa do skutecznego środka ochrony prawnej. Model sankcyjny pozbawiony jest zarówno kar pieniężnych, jak i instrumentów „miękkich", przez co nie zapewnia wystarczającego efektu prewencyjnego.

Całościowo system nadzoru nad przetwarzaniem danych w obszarze egzekwowania prawa wymaga zmian o charakterze systemowym – zarówno na poziomie instrumentów prawnych, jak i ich praktycznego stosowania.

Wnioski te znalazły odzwierciedlenie w wystąpieniu Prezesa UODO z 16 marca 2026 r., skierowanym do Ministra Spraw Wewnętrznych i Administracji oraz Ministra Sprawiedliwości, w którym wskazano potrzebę pilnych zmian legislacyjnych zapewniających pełną i skuteczną implementację dyrektywy (UE) 2016/680.